

RECEIVED
CENTRAL FAX CENTER

OCT 10 2006

REMARKS

Claims 1-20 stand rejected on prior art grounds. Claims 7 and 14 are herein cancelled. Thus, claims 1-6, 8-13 and 15-20 are all the claims presently pending in the application. Applicants respectfully traverse prior art rejections based on the following discussion.

I. Traversal of Examiner's Statement Indicating That A Common Knowledge Or Well-Known Statement Is Admitted As Prior Art.

The Examiner has indicated the Applicant did not challenge officially noticed facts cited in the previous Office Action and, therefore, those statements as presented are herein after prior art. Specifically, the Examiner indicates that the following statements are admitted as prior art:

“to schedule a meeting to discuss tasks (activities, deadlines, milestones, deliverables, etc.) that are missed overdue, late, in-trouble or the like wherein the meeting participants are the one or more resources responsible for and/or effected by the overdue tasks/activities wherein such meetings enable the team (project manager, sponsors, clients, etc.) to discuss how to address/rectify the situation (problem, issue, schedule constraints, etc.) in order to get the project back on track/schedule;” AND

“to identify (search, find) and assigning resources to project tasks/ activities (milestones, deliverables, etc.) that are missed, overdue, later, in-trouble or the like wherein project teams/managers identify and assign additional and/or alternative resources in order to get the project back on track/schedule.”

The Applicants traverse the admission of the above-quoted statements as prior art based on the following. On page 9 of the amendment submitted on May, 30, 2006, the Applicants traversed the rejection of all claims. On page 13, the Applicants indicated that the patentability of the dependent claims relied on both the patentability of their independent claims, but "also by virtue of the additional features of the invention they define." Thus, the Applicants did challenge the officially noticed facts that were offered by the Examiner in support of dependent claims 3, 10, and 17 as well as 6, 13 and 20.

II. The Prior Art Rejections

Claims 1-4, 7-11, and 14-18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Hung Chak Kuen Patrick, Secure Workflow Model (2001, Hung), hereinafter referred to as Hung, in view of Simmons, et al. Software Project Planning Associate (SPPA) as evidenced by at least Simmons et al., Software Project Planning Associate (SPPA): A Knowledge-Based Approach for Dynamic Software Project Planning and Tracking (2000), hereinafter referred to as Simmons.

Claims 5-6, 12-13, and 19-20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Hung in view of Simmons and further in view of Microsoft Project 2000 as evidenced by at least Pyron, et al., Using Microsoft Project 2000 – Special Edition (2000), hereinafter referred to as Pyron. Applicants respectfully traverse these rejections based on the following discussion.

In order to overcome these prior art rejections independent claims 1, 8 and 15 are amended herein to include the features (1) "wherein said encryption key ...is used to

automatically notify said appropriate resource of task responsibilities" and "wherein said monitoring comprises using a polling function to observe whether a resource is actively working on a task". The former feature is a feature that was previously presented in original claims 1, 8 and 15 and the later feature is a combination of features presented in claims 2, 7, 9, 14, and 16. Therefore, no new issues are raised that will require an additional search and the Applicants respectfully request that the amendments be entered.

The Applicants traverse the rejection of amended independent claims 1, 8 and 15 because the cited prior art references do not teach the following patentable features: (1) creating an encryption key for each one of said tasks, wherein said encryption key for each one of said tasks is used to automatically notify said appropriate resource of task responsibilities and allows access by said appropriate resource to said data source and said at least one design tool for a limited period of time;" and (2) "automatically monitoring work being performed on said tasks through a computerized network, wherein said monitoring comprises using a polling function to observe whether a resource is actively working on a task". Regarding amended independent claim 8, the cited prior art references also do not teach or suggest the feature that when a first task is prioritized as a prerequisite for a second task, the "creation of said encryption key for said second task is gated until completion of said first task."

More specifically, Hung is a thesis that describes a "Secure Workflow Model". Specifically, the system developed is a task-based document access model (i.e., access to documents is task based). Chapter 1 is an introduction setting out the security concerns with providing access to resources such as documents. Chapter 2 is an overview of

workflow concepts in general (e.g., on page 5 Hung discloses: workflow is a computer supported business process, a task is a workflow that involves a manipulation of resources, resources are “any kind of supply or support such as a document in either paper or electronic format”, etc.). An overview of the Hung’s model is found in chapter 4. Specifically, page 31 defines a secure workflow management system where each task represents a piece of work that needs to be done by an agent and where to accomplish the task the agent needs to “get certain access privileges (PR) (e.g., “read”, “write” and “read-write”) to a set of documents to ensure the security properties of integrity, authorization, availability, and separation of duties. Chapter 5 addresses a feature of the model termed “least privilege security”, in which the set of agents are given just enough privileges for accessing resources like documents to complete the workflows. Chapter 6 introduces a concept termed “failure resilience”, in which the concept of least privilege is relaxed to grant as few additional privileges as possible so as to guarantee completion of task execution even when some of the agents fail.

Simmons discusses the “Software Project Planning Associate (SPPA)” that can be accessed over the web and used “to assist a software project manager with initializing a software project plan, improving refining/improving a plan, organizing, staffing, scheduling,” etc. (see page 305, col. 1, para. 2). The SPPA uses tools, such as PAMPA, that can gather project information from any software development that can share directories over a network to a Microsoft windows client workstation, or PAMPA 2, that has the capability to operate from internet browsers. These tools can be used to monitor, measure, and calculate software project attributes, generate reports, etc. (see

page 307, col. 1, para. 3). A subsystem (Planning Intelligent Agents) helps keep track of project status, for example, the agent may determine that an activity is completed if by determining the current status of the activity corresponds to a final milestone that is stored in the knowledge base (see page 309, col. 2).

Pyron discloses that Microsoft Project 2000 is a scheduling and management tool for project managers and, specifically, provides tools for putting together a project schedule, assigning responsibilities, etc. (see Introduction page 1 of 2).

Whereas, the present invention relates to project planning and monitoring project progress, but has features that go beyond the project planning features disclosed in Hung, Simmons and Pyron. Namely, instead of simply providing tools that may be used by project managers for developing project plans, monitoring project progress, etc., the present invention, micromanages implementation of the design project plan through the use of encryption keys that integrate the project planner into the actual design tasks without the need of manual interventions (see paragraph [0036]). That is, the project planner receives information regarding each task that must be completed. This information includes an appropriate resource (i.e., the most appropriate designer for the task), the data source (i.e., the design data), at least one design tool (e.g., a specific design tool that is needed to complete the task) and the duration of the task (see paragraphs [0028-0029]). The tasks are prioritized and the project planner then creates a data structure for the tasks that includes this information in encrypted keys (see paragraph [0021] and Figure 5). Each key includes data, the designer's name, the start and end dates of the task and the tool to which the key provides access (see Figure 5). However,

if during the prioritizing, it is determined that a first task will gate a second task, an encryption key for the second task will not be created until after completion of the first task (see paragraphs [0029] and [0032]). If a task is completed during the time period allowed, the planner is updated and gated tasks are unlocked (i.e., encryption keys are created) (see paragraph [0032]). Once a task is unlocked, the designer can access the required data and tools. Thus, each encryption key notifies an assigned designer of the task and provides that designer with access to the specific design tool and data required to complete the task only during a limited period of time (see paragraphs [0021], [0030-0031], [0036]). Furthermore, once a user is logged on, the claimed invention uses a polling function (i.e., polling software) to actually monitor through the network the number of hours and minutes that a designer devotes to actively working on a particular task (in real time), not merely the amount of time a file is opened.

A. Regarding the feature in amended independent claims 1, 8 and 15 of "creating an encryption key for each one of said tasks, wherein said encryption key for each one of said tasks is used to automatically notify said appropriate resource of task responsibilities and allows access by said appropriate resource to said data source and said at least one tool for a limited period of time," the Office Action provides the following:

(1) "-creating an encryption key for each one of the tasks, wherein the encryption key allows access by the resource to the data source and at least one design tool (application, system, software, hardware, component, object, resource, etc.) for a limited period of time and wherein the creation of the encryption key for the second task is gated until completion of the first task (time-to-live, just-in-

time permissions, discretionary access control, mandatory access control, tasks-based authorization, temporal access control; Paragraphs 1-2, Page 13; Bullets 1-2, Page 14; Paragraphs 1-2, Page 20; Paragraph 1, Page 27; Bullets 1, 3, Page 34; Bullets 3-6, Page 35; "A secure workflow model grants the privilege for an agent to execute the task if all its input events have been accessed and all its depend tasks are completed.", Paragraph 3, Page 39; Last Paragraph, Page 41; Bullet 1, Page 54; Paragraph 2, Page 70; Bullets 1-2, Page 73; Figure 3.1). The Applicants respectfully disagree based on the following.

---Paragraphs 1-2, Page 13 refers to the concept of confidentiality and the process of using keys generally in order to limit access to workflow information to only agents (i.e., those persons assigned to execute a set of inter-dependent tasks, see paragraph 1, page 5) involved in the workflow. Thus, the cited portion does not disclose creating an encryption key for each task that allows access by a resource to a data source and at least one tool for a limited period of time.

---Bullets 1-2, Page 14 refer to authentication (i.e., requiring a user or computer to identify themselves to another computer) and authorization (i.e., a user identifies to the system the various functions which the user may undertake). Access control systems such as DAC and MAC (and not keys) are discussed by Hung as used for authentication and authorization (see page 14). For example, DAC controls the type of access that a subject has to an object (e.g., read, write, delete, copy, etc.). Whereas, MAC controls data flow between subjects and objects. Thus, page 18, line 12 indicates that DAC and MAC are only applied to control resources like databases and file systems. The details of

such access control systems are explained in section 3.2.1, pages 18-21. Thus, the cited portion does not disclose creating an encryption key for each task that allows access by a resource to a data source and at least one tool for a limited period of time.

---Specifically, paragraphs 1-2 on page 20 refer to role-based access control and team-based access control systems, which are based on the DAC approach and are, thus, only applied to control resources like databases and file systems. Paragraph 1 indicates that role-based access control limits access (i.e., the type of access, see discussion above) to resources based on a role (e.g., an organization unit, group, etc.) The activation criteria can be event-triggered and the deactivation criteria can be time-to-live (TLL). Those skilled in the art will recognize that TLL is a term of art referring to time until the access authority for users with that identified role expires. Paragraph 1 on page 20 further acknowledges that this type of access control is not present in per-task granularity. Paragraph 2 on page 20 indicates that team-based access control applies role-based access control concepts to collaborative environments. Team based has passive access lists like role-based and also has task-based permission activation and deactivation in accordance “with evolving context associated with progressing tasks” (e.g., just-in-time permissions). Those skilled in the art will recognize that “just-in-time” is a term of art that generally means “when needed” (e.g., when a condition is met). Again, nothing in the cited portions indicate that such access control is accomplished using encryption keys. Thus, the cited portion does not disclose creating an encryption key for each task that allows access by a resource to a data source and at least one tool for a limited period of time.

---Paragraph 1, Page 27 summarizes a conceptual model (task-based authorization (TBA)) of Thomas and Sandhu that describes modeling and management of the authorization of tasks in an information system. Words are listed e.g., dependencies, incorporation of controls, authorization expirations and deadline, etc. without explanation of their meaning. However, the summary does indicate that the TBA does not address the issues of authorization (i.e., user privileges, see page 14 of Hung) and availability (i.e., prevention of unauthorized withholding of information, see page 14 of Hung). Thus, the cited portion does not disclose creating an encryption key for each task that allows access by a resource to a data source and at least one tool for a limited period of time.

---Section 4.1 on page 34 is a summary of the secure workflow model (SWM) of Hung. The SWM of Hung is a multi-layered state machine with a workflow layer in which authorizations to access documents are granted to agents only during execution of an assigned task and are revoked when the task is finished, a control layer in which relevant events are generated only during task execution and a data layer in which document authorizations are granted and revoked from agents based on the occurrence of events during the task (see bullet 1). Bullets 3 of page 34 indicates that different security services can be applied to handle different security properties in the different layers (e.g., "the security service Public Key Infrastructure (PKI) can be applied to the Control Layer to handle the security properties of integrity in event transmissions. Further, the security service Discretionary Access Control (DAC) can be applied to the Workflow Layer and Data Layer to handle the security property of authorization for assigning/revoking tasks and documents to/from agents, respectively). Thus, while keys are mentioned to handle

security of integrity in event transmissions, the cited portion refers to the use of DAC to handle document authorization and, thus, does not disclose creating an encryption key for each task that allows access by a resource to a data source and at least one tool for a limited period of time.

Pages 35-38 provide a listing of defined security-relevant state variables with references to public keys to apply security services. However, the cited portion does not disclose creating an encryption key for each task that allows access by a resource to a data source and at least one tool for a limited period of time.

Last paragraph, Page 41 refers to the data layer and provides "An agent can only access a document with a specific privilege if and only if the document access privilege is granted to the agent and also it is needed to access the document with the privilege during the task execution. The secure workflow has to revoke the document access privilege from an agent if the document access privilege is no longer needed." Again, the cited portion does not disclose creating an encryption key that allows access by a resource to a data source and at least one tool for a limited period of time.

Section 4.1.5 describes the processing steps of the different security layers. For example, pages 48-49 describe the workflow initiation, task assignment, and task granted processes of the workflow layer. Followed by the task started and event generation process of the control layer (pages 50-51). These control layer processes trigger the access document, document granted and document revoked, process of the data layer. These data layer processes trigger the task completed process of the control layer, followed by the task revoked process of the data layer and the workflow completed

process of the workflow layer. Thus, the cited portion does not disclose creating an encryption key that allows access by a resource to a data source and at least one tool for a limited period of time.

Bullet 1 on page 73 provides that a specified period of time can be set within which a document process event can be executed. Bullet 2 indicates that a relative time period can be set to process the document (i.e., the agent can generate the events to process the document anytime between start and finish of the task). However, the cited portion does not disclose that it is an encryption key that is created that allows access for the limited period of time.

Consequently, as mentioned above Hung discloses a task-based document access model that specifically addresses security concerns related to accessing by multiple agents of documentary information during execution of inter-dependent tasks. No where in Hung does it teach or suggest a method step that "said encryption key for each one of said tasks is used to automatically notify said appropriate resource of task responsibilities and allows access by said appropriate resource to said data source and said at least one design tool for a limited period of time."

Firstly, no where in Hung does it disclose the use of encryption keys to automatically notify the appropriate resource of task responsibilities, etc. That is, the Office Action cites "dynamic assignment, work lists; Bullet 1, Page 6; Bullets 1-2, Page 112; "Each activity defined for the process must finish and then the agent who receives a notification has to act on it.", Paragraph 3, Page 114" of Hung as disclosing the feature of "automatically notifying resources of corresponding task responsibilities. The Applicants

respectfully disagree and furthermore submit that even if the feature of "automatically notifying" is disclosed, it is not accomplished through the use of a task specific encryption key. Bullet 1 of page 6 describes the role of a workflow coordinator, e.g., matching agents to tasks, adding work items to agent work list etc. It handles communications between the system and the agents etc. Nothing in the cited portion indicates that notification is automatic and, more importantly, communication between the system and the agents are disclosed as being handled through the coordinator not via an encryption key. Section 7.2.1, which includes the cited bullets on page 112, discusses the IBM MQ Series Workflow which modeler which assigns agents of an organization to one of several levels based on a security policy (e.g., a security clearance). Then, for a specific process that needs to be executed, the security level is defined such that any agent or the specific agent that is assigned to perform that process must have that defined security level. Section 7.2.1, which includes the cited portion of page 114, refers to the data layer of the modeler with a process-based data structure and access privilege and, specifically, with a temporal access control (TAC) (not an encryption key) that grants privileges to access specific documents in a specific manner for a specified time.

Secondly, page 13, paragraph 1 refers to a public key infrastructure generally to limit access to sensitive information to only those agents involved. Sections 4.1-4.1.3 refers to the three layers of the secure workflow model of Hung and specifically, the use of keys to handle security services in the control layer. However, keys are disclosed as applied to the control layer to handle the security of integrity in event transmissions, whereas, DAC is disclosed as being applied to the Workflow Layer and Data Layer to

handle the security property of authorization for assigning/revoking tasks and documents to/from agents, respectively. Thus, although keys are used in Hung for security purposes, DAC and not keys are used to actually control access to documents.

Finally, the Office Action indicates that Hung discloses "at least one design tool (application, system, software, hardware, component, object resources, etc.)" However, the cited portions of Hung do not include an application, system, software, hardware, component, object, and resources, much less a design tool, disclosed. Furthermore, while paragraph 1 on page 111 of Hung does indicate that the modeler may define IT resources (such as programs) that are needed in the process, nothing in the cited portions of Hung disclose, teach or suggest that access authorization to such programs is specified along with access authorization to the documents, much less that such a program access authorization is specified within an encryption key that is the same encryption key that allows access to the data source.

B. Regarding the feature in independent claims 8 of "creation of said encryption key for said second task is gated until completion of said first task."

The Office Action appears to cite, paragraph 3, page 39 of Hung as disclosing that "creation of said encryption key for said second task is gated until completion of said first task". The Applicants respectfully disagree. The cited portion of Hung the refers to the workflow layer and provides "A secure workflow model grants the privilege for an agent to execute the task if all its input events have been accessed and all it depend tasks are completed." While this cited portion does indicate that the granting of a privilege is conditional upon completion of a depend task, it does not indicate that the privilege is

granted via an encryption key, much less that the actual creation of the encryption itself is gated.

The Office Action also appears to be citing paragraph 2, page 70 of Hung as teaching this feature. The Applicants respectfully disagree. The cited portion refers to temporal access control which is used to monitor the integrity of document accesses. That is, "the set of documents that will be accessed by an agent during the execution of a task can also be pre-defined at specification time by Temporal Access Control (TAC). . .

.. The document access is temporal, that is, if an agent needs to access multiple document, there is a partial order in which these order in which these documents are requested. Thus, one document access event is expected to occur before or after another document access event (or, end of the task)." That is, a user may be expected to access one document before accessing another document. Note that resolution of conflicts of concurrent access by more than one agent to the same document is out of the scope of Hung (see page 70, lines 20-21). Thus, indicate that document access is ordered, it does not indicate that the access to each document is granted via encryption keys, much less that the actual creation of an encryption key to access one document is gated until another document has been accessed.

C. Regarding the feature in independent claims 1, 8 and 15 of "automatically monitoring work being performed on said tasks through a computerized network, wherein said monitoring comprises using a polling function to observe whether a resource is actively working on a task"

The Office action cites "workflow monitoring, workflow path; monitoring workflow state and transitions; Paragraph 1, Page 33; Pages 35-38; Bullet 1, Page 104 of Hung as well as "PAMPA; Column 1, Last Paragraph, Page 306; Section 3, Page 307; Section 5.2, Page 309" of SPPA as teaching the feature of "automatically monitoring work being performed on the tasks through a computerized network. The Applicants respectfully disagree. The cited portions of Hung refer to monitoring completion of tasks in a workflow path in which execution of some tasks is dependent upon completion of other tasks. They do not disclose monitoring the work being performed on a task by observing whether a resource is actively working on a task. The cited portions of SPPA refer to the general functions including intelligent agents that track project status (e.g., determine compliance with milestones, current phase of a project, problems with software, etc.) and PAMPA which monitors, measures and calculates software project attributes. Thus, the cited portions of the SPPA refer to monitoring of attributes of the project itself, not actually monitoring the work being performed by observing whether a resource is actively working on a task.

The Office Action cites "workflow state and transition monitoring and control; event-driven activity execution, project monitoring, execution control, pattern of operation, context/task permission activation etc.; Bullet 1, Page 7; Paragraph 1, Page 16; Last Paragraph, Page 20; Paragraph 3, Page 39" of Hung as teaching the feature of "wherein monitoring further comprises observing whether a resource is actively working on a task ...". Again, the cited portions of Hung refer to monitoring completion of tasks in a workflow path in which execution of some tasks is dependent upon completion of

RECEIVED
CENTRAL FAX CENTER
OCT 10 2006

other tasks. They do not disclose monitoring the work being performed on a task by observing whether a resource is actively working on a task.

The Office Action cites "PAMPA; Abstract; Section 3, Page 307; Figure 1" of SPPA as disclosing a polling function "to proactively monitor and mange the project (e.g., the system tracks/monitors the project's progress/status, ...". Again, the cited portions of the SPPA refer to monitoring of project attribute, not observing whether a resource is actively working on a task. Furthermore, the monitoring of project attributes is in SPPA is accomplished through the use of intelligent agents, not through a polling function.

D. Conclusion

In view of the foregoing, amended independent claims 1, 8 and 15 are patentable over the cited prior art. Further, dependent claims 2-6, 9-13 and 16-20 are similarly patentable, not only by virtue of their dependency from a patentable independent claim, but also by virtue of the additional features of the invention they define. Moreover, the Applicants note that all claims are properly supported in the specification and accompanying drawings, and no new matter is being added. In view of the foregoing, the Examiner is respectfully requested to reconsider and withdraw the rejections.

II. Formal Matters

With respect to the rejections to the claims, the claims have been amended, above, to overcome these rejections. In view of the foregoing, the Examiner is respectfully requested to reconsider and withdraw the rejections to the claims.

RECEIVED
CENTRAL FAX CENTER

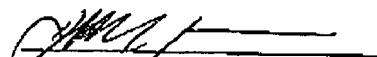
OCT 10 2006

In view of the foregoing, Applicants submit that claims 1-6, 8-13 and 15-20, all the claims presently pending in the application, are patentably distinct from the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary. Please charge any deficiencies and credit any overpayments to Attorney's Deposit Account Number 09-0456.

Respectfully submitted,

Dated: 10/10/06



Pamela M. Riley
Registration No. 40,146

Gibb I.P. Law Firm, LLC
2568-A Riva Road, Suite 304
Annapolis, MD 21401
Voice: (410) 573-0227
Fax: (301) 261-8825
Customer Number: 29154